REMARKS

Rejection Under 35 U.S.C. 112

Claim 6 was rejected under 35 U.S.C. 112 which states that "[t]he specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention." The pre-amendment claim 6 read, "[t]he device of claim 4, wherein the electrical signal is an address." In reference to claim 6, the Office Action states that "[t]here is insufficient antecedent basis for this limitation in the claim." To conform to this rejection, Applicants have amended claim 6 to properly reference claim 5, not claim 4. As amended, Applicants respectfully submit that claim 6 overcomes the aforementioned rejection under 35 U.S.C. 112.

Rejections Under 35 U.S.C. 101

Claims 17-23 were rejected under 35 U.S.C. 101 because "a computer readable storage medium comprising computer readable code" is directed to non-statutory subject matter. Referring to this rejection, the Office Action states that "[g]enerally, functional descriptive material, such as a computer program, is statutory when it is stored on a tangible computer readable medium. However, in the present application the specification doesn't define 'computer readable medium', so 'computer readable medium' could be, for example, paper or various transmission media." To comply with the foregoing rejections, Applicants have amended claim 17 to read "[a] computer readable storage medium comprising computer readable code *executable by a digital processing apparatus*, the computer readable code configured to..." [emphasis added]. Applicants respectfully assert that the amended language of claim 17 removes the subject matter from the realm of transmission media and places claims 17-23 in compliance with 35 U.S.C. 101.

Rejections Under 35 U.S.C. 102

Claims 1-30 were rejected under 35 U.S.C. 102(b) as being anticipated by Trust Computing Platform Alliance (TCPA), "Main Specification Version 1.1b" (hereinafter "the

TCPA Specification"). The TCPA Specification declares itself as "an industry specification that enables trust in computing platforms in general." See page 1 of the TCPA Specification. The TCPA Specification "defines a trusted *Subsystem* that is an integral part of each platform, and provides functions that can be used by enhanced operating systems and applications. The Subsystem employs cryptographic methods when establishing trust, and while this does not in itself convert a platform to a secure computing environment, it is a significant step in that direction." See page 1 of the TCPA Specification.

In light of the rejections under 35 U.S.C. 102(b), a review of the present invention may help clarify the novelty of Applicants' claims over the reference under consideration. Referring to paragraphs [0003], [0004], [0007], [0008], and [0037]–[0044], a secure computing module (often referred to in the specification as "SCM") transacts secure functions with one or more Computing Modules. A Computing Module may be an excluding computing module (often referred to in the specification as "ECM").

The excluding computing module is designed to exclude all secure function transactions between the secure computing module and other Computing Modules (i.e. non-excluding computing modules). Unfortunately, many Computing Modules, such as legacy services and applications, are not designed to operate through an excluding computing module. Computing Modules that cannot transact secure functions through the excluding computing module are non-conforming computing modules (often referred to in the specification as "NCM"). The non-conforming computing module may be a legacy Computing Module that was created before the excluding computing module.

To maintain proper security, a secure data processing device with an excluding computing module that is transacting secure functions with a secure computing module cannot also have a non-conforming computing module that is transacting secure functions with the secure computing module. If the non-conforming computing module attempts to transact secure functions directly with the secure computing module, the non-conforming computing module will be denied access to transact the secure functions. Alternatively, if the non-conforming computing module transacts secure functions directly with the secure computing module, the excluding computing module will detect the secure function transactions. The excluding

computing module may determine that the security of the secure computing module is compromised and stop secure function transactions with the secure computing module, preventing the excluding computing module from transacting secure functions to protect sensitive data.

As such, the present invention provides a solution that enables both an excluding computing module and a non-conforming computing module to transact secure functions with a single secure computing module. The present invention accomplishes this by a secure computing module that receives a communication from a computing module which may include a non-conforming computing module or an excluding computing module. Upon receiving the communication, the secure computing module identifies the computing module (which may be done using a cryptographic key solution and/or an address based system) and sets the context of the secure computing module to the appropriate context—i.e. a context for an excluding computing module or for a non-conforming computing module. By doing so, the secure computing module is able to "adapt" to a required context and securely communicate with both an excluding computing module and a non-conforming computing module (i.e. legacy services and applications not designed to operate through or in conjunction with the excluding computing module), thereby overcoming the previous inability for a secure computing module to communicate with both excluding computing module and non-conforming computing module.

According to Applicants reading of the TCPA Specification, the reference provides a solution for secure data transfer distinct from that of the present invention. For example, the TCPA Specification provides a platform subsystem that enables an entity to "deduce whether the state of the computing environment on that platform is acceptable and perform some transaction with that platform." The TCPA Specification states that "other functions" (the Support Services, or SS) do not have to be trusted to function properly." Trusted Support Services or TSS is defined as "functions and data that are common to all types of platform, which are not required to be trustworthy..." As such, the TCPA Specification facilitates functions between an entity and a platform where the functions are determined to be acceptable or are already deemed as acceptable.

The present invention, on the other hand, provides a solution that enables both an excluding computing module and a non-conforming computing module to transact secure functions with a single secure computing module. As explained in the background section of Applicants' application, an excluding computing module and a non-conforming computing module are operationally mutually exclusive from a single secure computing module stand point. For this reason, the present secure computing module "adapts" to the context of the computing module with which computing module the secure computing module is communicating. As such, Applicants respectfully submit that the TCPA Specification does not teach or enable the contextually dynamic secure computing module of the present invention.

Additionally, Applicants respectfully assert that a non-conforming computing module is not analogous to the already-acceptable Support Services (TSS) of the TCPA Specification as cited in the Office Action due to the operationally mutually exclusive nature of an excluding computing module and an non-conforming computing module. Indeed, applicant respectfully asserts that not only does the present invention include elements distinct from the TCPA Specification, but that the present invention is directed toward solving problems not considered by the TCPA Specification.

Conclusion

In order to further clarify the present invention, Applicants have amended independent claims 1, 8, 17, 24, and 30. Applicants submit that the amendments sufficiently clarify the claimed subject matter and place the claims and their dependent claims in condition for allowance. In the event any questions remain, the Examiner is respectfully requested to initiate a telephone conference with the undersigned.

Respectfully submitted,

Date: June 11, 2007

__/Brian C. Kunzler/___

Kunzler & Associates
8 E. Broadway, Suite 600
Salt Lake City, Utah 84111
Telephone: 801/994-4646

Brian C. Kunzler
Reg. No. 38,527
Attorney for Applicant